

(19) 日本国特許庁(JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2001-136159

(P 2001-136159A)

(43) 公開日 平成13年5月18日 (2001.5.18)

(51) Int. Cl. 7	識別記号	F I	テーマコード* (参考)
H 0 4 L	9/08	H 0 4 B	7/24 B 5C064
H 0 4 B	7/24	H 0 4 H	1/00 E 5J104
H 0 4 H	1/00		H 5K067
H 0 4 N	7/173 6 2 0	H 0 4 N	7/173 6 2 0 Z
		H 0 4 L	9/00 6 0 1 B
審査請求	未請求	請求項の数 1 1	OL (全 1 1 頁)

(21) 出願番号 特願平11-311651

(22) 出願日 平成11年11月1日 (1999. 11. 1)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 赤地 正光

東京都品川区北品川6丁目7番35号ソニー株式会社内

(74) 代理人 100082740

弁理士 田辺 恵基

F ターム (参考) 5C064 BA01 BB05 BB07 BC10 BC17
BC22 BD08

5J104 AA01 AA16 BA03 EA01 EA04

JA03 NA02 PA04

5K067 AA30 BB00 CC12 CC13 DD17

EE07 HH36

(54) 【発明の名称】 情報伝送システム及び方法、送信装置及び受信装置

(57) 【要約】

【課題】 様々な受信制御を行い得る情報伝送システムを得る。

【解決手段】 受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにした。

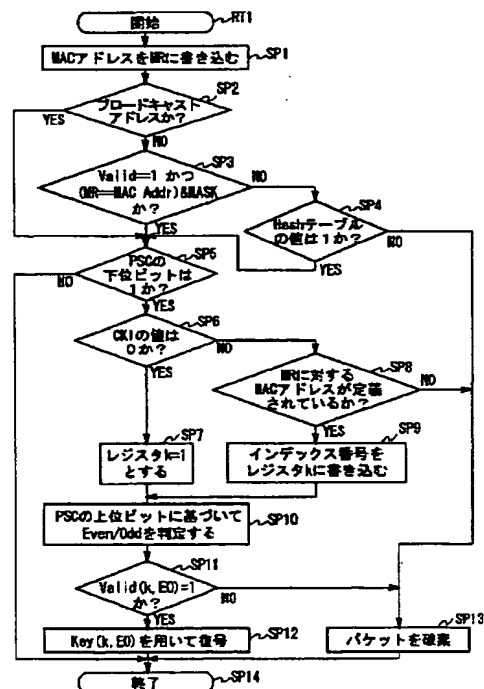


図6 復号処理

【特許請求の範囲】

【請求項 1】送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送システムにおいて、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する上記送信装置と、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する上記受信装置とを具えることを特徴とする情報伝送システム。

【請求項 2】上記送信装置は、上記複数の上記受信装置全てにデータを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信し、上記受信装置は、受信した上記データに上記同報アドレスが付せられているとき、当該データを復号することを特徴とする請求項 1 に記載の情報伝送システム。

【請求項 3】上記受信装置は、上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行うことを特徴とする請求項 1 に記載の情報伝送システム。

【請求項 4】上記送信装置は、上記受信装置に対して個別にデータを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化し、

上記受信装置は、当該受信装置に対して個別に送信されたデータを、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて復号するとともに、任意のグループの上記受信装置間に対して送信されたデータを、上記共通鍵を用いて復号することを特徴とする請求項 1 に記載の情報伝送システム。

【請求項 5】送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共

通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する送信ステップと、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する受信ステップとを具えることを特徴とする情報伝送方法。

10 【請求項 6】それぞれ固有のアドレスを有する複数の受信装置にデータを送信する送信装置において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信することを特徴とする送信装置。

20 【請求項 7】上記複数の上記受信装置全てに上記データを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信することを特徴とする請求項 6 に記載の送信装置。

【請求項 8】上記受信装置に対して個別に上記データを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化することを特徴とする請求項 6 に記載の送信装置。

30 【請求項 9】所定の送信装置から送信されたデータを受信して復号する受信装置において、

受信した上記データに付せられたアドレスと、当該受信装置固有のアドレスとが一致したとき、又は、受信した上記データに付せられた、複数の上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と当該アドレスの共通部分の範囲を指定するアドレス範囲情報とに基づいて、固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号することを特徴とする受信装置。

40 【請求項 10】受信した上記データに所定の同報アドレスが付せられているとき、当該データを復号することを特徴とする請求項 9 に記載の受信装置。

【請求項 11】上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行うことを特徴とする請求項 9 に記載の受信装置。

【発明の詳細な説明】

50 【0001】

【発明の属する技術分野】本発明は情報伝送システム及び方法、送信装置及び受信装置に関し、例えば衛星を介して情報を伝送する情報伝送システムに適用して好適なものである。

【0002】

【従来の技術】従来デジタル衛星放送システムにおいては、受信契約を行った正当な受信者のみが放送を受信し得る限定受信機構（CA：Conditional Access）が用いられている。

【0003】かかる限定受信機構においては、受信契約を行った受信者に対して予め所定の秘密鍵を渡しておく。送信側はこの秘密鍵を用いて放送データを暗号化し、放送衛星を介して送信する。そして受信者は秘密鍵を用いて受信波の暗号化を解除することにより、受信契約を行った受信者のみが放送を視聴し得るようになされている。

【0004】

【発明が解決しようとする課題】ここで近年、デジタル衛星放送システムを用いてデータ伝送を行う、衛星データ伝送システムが考えられている。衛星回線は電話回線やISDN回線等比べてその通信速度が速いため、大容量データを短時間で伝送することができという利点がある。

【0005】この衛星データ伝送システムにおいて、各受信者に対して個別のデータを伝送する個別通信（以下、これをユニキャストと呼ぶ）に加えて、全ての受信者に対して同一のデータを伝送する同報通信（以下、これをブロードキャストと呼ぶ）や、任意の受信者グループに対して同一のデータを伝送するグループ通信（以下、これをマルチキャストと呼ぶ）等の様々な受信制御を行うことができれば、衛星データ伝送システムの使い勝手がより一層向上すると考えられる。

【0006】ところがかかる限定受信機構においては、全受信者が常に同じ情報を受信して視聴することを前提として設計されているため、ユニキャストやマルチキャスト等の受信制御を行い得ないという問題があった。

【0007】本発明は以上の点を考慮してなされたもので、様々な受信制御を行い得る情報伝送システム及び方法、送信装置及び受信装置を提案しようとするものである。

【0008】

【課題を解決するための手段】かかる課題を解決するため本発明においては、送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレ

スの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにした。

【0009】任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信し、受信装置では固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較し、比較結果が一致したとき当該データを復号するようにしたことにより、簡易な構成で様々な受信制御を行い得る。

【0010】

【発明の実施の形態】以下図面について本発明の一実施の形態を詳述する。

【0011】（1）衛星データ伝送システムの全体構成図1において、1は全体として本発明を適用した衛星データ伝送システムを示し、送信側システム2、衛星3、及び複数の同一構成でなる受信側システム4で構成される。送信側システム2と各受信側システム4とはそれぞれインターネット5を介して接続されている。また送信側システム2を管理するサービスプロバイダと各受信側システム4を所有する受信者との間では、予め当該衛星データ伝送システム1についての利用契約が結ばれている。

【0012】送信側システム2においては、当該送信側システム2全体を制御する制御装置10、回線接続装置11、データサーバ12及び送信処理装置13がローカルネットワーク14を介して接続されている。

【0013】制御装置10は、受信側装置4が有する情報処理装置22から送信されたデータ読出要求を、回線接続装置11を介して受信する。そして制御装置10はデータ読出要求に応じて、データサーバ12或いはインターネット5上のデータサーバ（図示せず）からデータを読み出し、送信処理装置13に供給する。

【0014】ここで送信処理装置13は、受信側装置4の各情報処理装置22に付せられた固有の識別番号であるMAC（Media Access Control：メディアアクセス制御）アドレスと、当該MACアドレスに対応して設定された秘密鍵とを記述した暗号鍵対応表を有している。そして送信処理装置13は秘密鍵対応表に基づいて、読み出されたデータをデータ送信先の情報処理装置22のMACアドレスに対応した秘密鍵を用いてデータを暗号化する。また送信処理装置13は、ブロードキャストとして全ての情報処理装置22に送信するデータについて、当該データのCKI（Common Key Indicator、後述）の

値を”0”とするとともに、所定の共通鍵を用いて暗号化する。そして送信処理装置13は、暗号化したデータをDVB (Digital Video Broadcasting) データ放送仕様に定める形式でパケット化し、アップリンク波S2として送信15を介して衛星3に送信する。

【0015】衛星3はアップリンク波S2を受信して増幅し、ダウンリンク波S3として地上の受信側システム4に向けて再送信する。

【0016】受信側システム4においては、受信装置21、回線接続装置23、及び、例えばパーソナルコンピュータ等となる複数の情報処理装置22が、ローカルネットワーク24を介して相互に接続されている。

【0017】受信装置21は、受信アンテナ20を介して受信したダウンリンク波S3に対して復調処理及び後述する復号処理を行うことにより、情報処理装置22に向けて送信されたデータを復号し、ローカルネットワーク24を介して、当該情報処理装置22に供給する。

【0018】また情報処理装置22は、ユーザによってデータの読出要求操作が入力されると、これに応じてデータの読出要求を回線接続装置23及びインターネット

5を介して送信側システム2に送信する。

【0019】(2) 受信装置の構成

次に、受信側システム4の受信装置21を図2を用いて説明する。

【0020】受信装置21においては、当該受信装置21全体を制御するCPU (Central Processing Unit) 30に、バス39を介してフロントエンド部31、分離部32、受信フィルタ33、復号部34、チェッカ35、バッファ36、鍵テーブル37及びインターフェイス部38が接続されている。

【0021】フロントエンド部31は、受信アンテナ39を介して受信したダウンリンク波S3を復調し、データストリームD31としてデマルチプレクサ32に供給する。デマルチプレクサ32は、PID (Packet ID) に基づいて、データストリームD31から必要なパケットのみを分離して受信フィルタ33に供給する。受信フィルタ33は、デマルチプレクサ32から供給されたパケットのペイロード内容を調べ、データ復号処理に不要なパケットを破棄する。

【0022】復号部34は後述する復号処理に基づいて動作し、情報処理装置22 (図1) のMACアドレスを検索キーにして鍵テーブル28に問い合わせを行い、当該鍵テーブル28から復号鍵を取得する。そして復号部34は、取得した復号鍵を用いてデータストリームD31を復号し、復号データD34としてチェッカ35に供*

($\sim (MR_i \wedge MAC_i(k))$) & MASK_i(k) (1)

【0030】なる演算を $0 \leq i \leq 47$ なる範囲で全てのビットに対して行い、この結果が全て”0”である場合にMACアドレスが合致したとするものである。

【0031】これはすなわち、マスクが”1”であるビ

*給する。

【0023】チェッカ35は、復号データD34に対して復号処理が正常に行われたか否かの検査を行い、正常に復号されたパケットのみをバッファ36に供給する。そしてバッファ36はCPU30の要求に応じて、復号データD34をバス39を介してインターフェイス部38に読み出す。インターフェイス部38は、復号データD34をローカルネットワーク24 (図1) を介して情報処理装置22に供給する。

【0024】かくして受信装置21はダウンリンク波S3を受信し、情報処理装置22向けに供給されたデータのみを取り出して当該情報処理装置22に供給する。

【0025】(3) デジタルストリームの復号処理

デジタルストリームD31は、図3に示すように、ペイロードの先頭にパケットヘッダ情報が付加されるとともに、ペイロードの末尾にスタッフィングバイト (無効バイト) 及びCRC (Cyclic Redundancy Code : 巡回冗長符号) が付加され、DVBデータ放送仕様に定めるセッションとして処理可能な形態 (Datagram-section) にカプセル化されて構成される。ここでMACアドレス#6とは、MACアドレスの最上位ビットをBit47、最下位ビットをBit0としたときの、Bit7からBit0を含むバイト (8bit) を意味する。

【0026】復号部34においては、まず受信したデータストリームD31の各パケットに記述されたMACアドレスと鍵テーブル37とに基づいて、当該パケットを受信すべきか否かを弁別する。

【0027】ここで本発明による受信装置21は、かかるパケット弁別処理において、MACアドレスにおける比較すべきビット位置を指定するマスクビット処理と、MACアドレスをより少ないビット数の数値に変換し、これを用いてパケットの弁別を行うMACアドレス変換処理と、特定のMACアドレスを有するパケットを無条件で通過させるMACアドレス通過処理とを実行する。

【0028】マスクビット処理は、セッションヘッダに記述されたMACアドレスと鍵テーブル37のMACアドレスの比較演算による状態判定に、マスクビットと比較演算結果の論理積演算を付加するものであり、で、排他論理和を \wedge 、論理積を&で表し、セッションヘッダ記載のMACアドレスをMR、鍵テーブルk番めのMACアドレスをMAC(k)、ビットの重みを1と表すすると、各ビット毎に

【0029】

【数1】

ットにおいてのみMRとMACアドレスの比較を行うということである。このマスクビットとMR及びMACアドレスの比較操作との関係を図4に示す。

【0032】図4の場合、マスクビットはD0～D3ま

でが”0”であり、D4～D47は”1”である。かかるマスクビットを用いてMACアドレスの照合を行う場合、マスクビットが”1”であるD4～D47の区間において、MACアドレスとMRが同一であることがMACアドレスの合致条件であり、マスクビットが”0”であるD0～D3の区間は、MACアドレスとMRが同一でなくてもかまわない。このようにマスクビットを用いてMACアドレスの一部のみを照合することにより、それぞれ異なるMACアドレスを有する任意の情報処理装置22に対して同一のパケットを配信するマルチキャスト（グループ通信）を行うことができる。またマスクビットを全て”1”、即ち”0xFFFFFFFF”とすることにより、MACアドレス全てのビットに対して照合が行われ、ユニキャスト（個別通信）を行うことができる。

【0033】ここで、マスクビットを用いてマルチキャストを行う場合、各情報処理装置22のMACアドレスに共通部分が存在することが前提となるが、そのように情報処理装置22を揃えることは難しく、またシステムを運用する際の柔軟さを欠くことにもなる。この場合、実際の情報処理装置22のMACアドレスとパケットヘッダに記述されるMACアドレスとの対応表に基づいて、パケットヘッダを書き換えて疑似的にMACアドレスの共通部分を作り出すようにすればよい。

【0034】MACアドレス変換処理は、入力したMACアドレスに対してある種の計算式（ハッシュ関数）による演算を行い、48ビット以下のビット数に縮小した数値を得、これをキーにして通過させるか否かを記述したテーブル（ハッシュテーブル）を検索するものである。このビット数の縮小は、ハッシュテーブルを小さくするためである。ハッシュ関数は入力されるMACアドレスをよく分散させるような関数であれば何でも良く、例えばMACアドレスのCRCを求め、この上位6ビットをpとし、Pass(p)が”1”であれば通過させ、例えば”0”であれば破棄する。ここでpassは $2^6 = 64$ ビットのテーブルである。このようにハッシュ関数を用いてMACアドレスのビット数を縮小することにより、復号部34の回路規模を小さくすることができる。

【0035】またMACアドレス通過処理は、パケットのヘッダに記述されたMACアドレスが所定の同報通信用のアドレスである場合、鍵テーブルの状態に関わらず通過させるというものであり、例えばパケットのヘッダ記載のMACアドレスが”0xFFFFFFFF”（このアドレスをブロードキャストアドレスと呼ぶ）であれば常に同報通信（ブロードキャスト）とみなしてこれを通過させる。本発明においては、かかるMACアドレス通過処理をマスクビット処理及びMACアドレス変換処理に先行して実行する。これによりパケットヘッダ記載のMACアドレスがブロードキャストアドレスである場合鍵テーブルの検索が不要になり、処理速度が向上するという効

果がある。

【0036】かくして復号部34は、パケットのヘッダに記述されたMACアドレス、情報処理装置21のMACアドレス、及びマスクビットに基づいてパケットの弁別を行う。

【0037】続いて復号部34は、弁別されたパケットが暗号化されているかを検出する。そしてパケットが暗号化されているときは、復号鍵を鍵テーブルより取り出して復号処理を行うが、同報通信においては複数のMACアドレスで共用する復号鍵である共通鍵を具備する必要がある。

【0038】本発明による受信装置21では、共通鍵を使用するか否かを、例えばセクション6バイト目の最上位ビット（図3の2行めの第2番目のバイトのD7）を用いて判断する。これを本発明ではCKI（Common Key Indicator）と呼ぶ。そしてCKIが”1”であれば、MR、MACアドレス及びマスクビットによって鍵テーブルから抽出される個別鍵を使用し、CKIが”0”であれば、鍵テーブルの設定にかかわらず共通鍵を使用すると定める。ここで、DVBデータ放送仕様においてはCKIはreservedとされており、値として”1”をとることになっている。共通鍵は個別鍵に比べてより特殊な処理方法であると考えられるので、CKIが”0”である場合に共通鍵を使用すると定めることで、DVBデータ放送仕様との仕様を一致することができる。

【0039】共通鍵は特定の記憶領域を用意しても良いが、鍵テーブル中の特定の行のデータを兼用すれば処理が個別鍵と共通化でき、記憶領域も有効に利用できるものでより望ましい。この特定の行としてより好ましくは先頭の行、即ち第1行を指定する。鍵テーブルの行数nがいくつであれ必ず第1行めは存在するので、このようにすればnの値が異なる受信装置であっても処理手順を変えることなく共通鍵の記憶又は取り出しを行うことができる。

【0040】図5は鍵テーブルの構成を示し、MACアドレス#1は鍵テーブルの第1番行に記述されたMACアドレスを、マスク#1はMACアドレス#1に対応するマスクビットを、K_{1Even}、K_{1odd}は各々MACアドレス#1に対応づけられたEven/Oddの鍵データを意味しており、使用する暗号形式に応じたビット幅mを持つ。鍵テーブルは上記と同様の構造を複数（n個）持っている。この最大数は鍵テーブル28が持ちうる回路規模から上限が決定される。

【0041】MACアドレスと鍵データはそれぞれ独立したValidフラグを有しており、これにより個別に値が有効であるか無効であるかを管理することができるようになされており、当該Validフラグを、MACアドレス弁別に流用することも可能になる。また、鍵テーブルは各行毎に独立したValidフラグを有してい

るため、当該鍵テーブルは空行（無効な行）を含んでいても良く、これにより一時的に特定の行の情報を無効にしたい場合、単にMACアドレスのValidビットを”0”にするだけでよく、高速な処理のために好適である。

【0042】復号部34は、かくして得られた復号鍵を用いてパケットの復号を行う。

【0043】（4）復号処理手順

次に、デジタルストリームの復号処理手順を図6の流れ図に示しながら説明する。

【0044】復号部34はRT1で処理を開始し、ステップSP1において、パケットヘッダに記述されている48bitのMACアドレスをレジスタMRに読み込み、次のステップSP2に進む。

【0045】ステップSP2において、復号部34はレジスタMRの値がブロードキャストアドレス（0xFFFFFFF）に等しいか否かを判断する。ステップSP2において肯定結果が得られた場合、このことはレジスタMRの値がブロードキャストアドレスに等しいこと、すなわち当該パケットがブロードキャストパケットであることを表しており、復号部34はステップSP3及びSP4をスキップし、ステップSP5に進む。

【0046】これに対してステップSP2において否定結果が得られた場合、このことはレジスタMRの値がブロードキャストアドレスに等しくないこと、すなわち当該パケットがブロードキャストパケットではないことを表しており、復号部34はステップSP3に進む。

【0047】ステップSP3において、復号部34は鍵テーブル37内に、Validビットが”1”（すなわち有効状態）であるとともに、マスクビットが”1”である区間の全ビットにおいてレジスタMRとMACアドレスとが等しい行が存在するか否かを、（1）式に基づいて鍵テーブルを#1行から順に各行検索する。

【0048】ステップSP3において肯定結果が得られた場合、このことは有効状態かつマスクビットが”1”である区間の全ビットにおいてレジスタMRとMACアドレスとが等しい行が存在したことを表しており、復号部34はステップSP5に進む。

【0049】これに対してステップSP3において否定結果が得られた場合、このことは有効状態かつマスクビットが”1”である区間の全ビットにおいてレジスタMRとMACアドレスとが等しい行が存在しないことを表しており、復号部34はステ4に進む。

【0050】ステップSP4において、復号部34は、ハッシュ関数を用いてパケットヘッダに記載のMACアドレスからハッシュ値を生成し、当該ハッシュ値を用いて所定のハッシュテーブルを検索し、ハッシュ値に対応するビットが”1”であるか否かを判断する。

【0051】ステップSP4において否定結果が得られた場合、このことはハッシュテーブルのビットが”0”

であり、当該パケットは受信装置21が受信すべきパケットではないことを表しており、復号部34はステップSP13に進み、当該パケットを破棄し、ステップSP14で処理を終了する。

【0052】これに対してステップSP4において肯定結果が得られた場合、このことはハッシュテーブルのビットが”1”であり、当該パケットは受信装置21が受信すべきパケットであることを表しており、復号部34はステップSP5に進む。

10 【0053】ステップSP5において、復号部34は、パケットヘッダにおけるPSC（Payload Scrambling Control）（図3）の下位ビットの値に基づいて、当該パケットが暗号化されているか否かを判断する。ステップSP5において否定結果が得られた場合、このことは下位ビットが”0”であること、すなわち当該パケットが暗号化されていないことを表しており、復号部34はステップSP14へ進み、暗号解除処理を行わずにパケットを後段のチェッカ35に送出し処理を終了する。

20 【0054】これに対してステップSP5において肯定結果が得られた場合、このことは下位ビットが”1”であること、すなわち当該パケットが暗号化されていることを表しており、復号部34はステップSP6に進む。

【0055】ステップSP6において、復号部34は、パケットヘッダにおけるCKI（図3）の値に基づいて、当該パケットが共通鍵を用いて暗号化されているか否かを判断する。ステップSP6において肯定結果が得られた場合、このことはCKIが”0”であること、すなわち当該パケットが共通鍵を用いて暗号化されていることを表しており、復号部34はステップSP7へ進み、鍵の索引番号を記憶するレジスタkに共通鍵を示す”1”を代入し、ステップSP10に進む。

30 【0056】これに対してステップSP6において否定結果が得られた場合、このことはCKIが”1”であること、すなわち当該パケットが個別鍵を用いて暗号化されていることを表しており、復号部34はステップSP8に進む。

【0057】ステップSP8において、復号部34は鍵テーブルを（1）式に基づいて各行順次検索し、MRに合致するMACアドレスが鍵テーブル上に存在するか否かを判断する。ここで、ステップSP4におけるハッシュテーブルによる弁別では受信すべきではないパケットもたまたまハッシュ値が合致すれば通過させてしまうが、このようなパケットは当該ステップSP8にて再度弁別されるため、誤って復号処理されることはない。ちなみに、暗号化されていないパケットはステップSP8を通過しないので、これは後段回路あるいは情報処理装置22にて破棄する。

50 【0058】鍵テーブルの探索は、当該鍵テーブルの第1行から順に行われ、最初に合致するまで照合が繰り返される。ここで、有効なアドレスとは図5に示すVal

idビットが活性状態であるものである。例えばValidビットが”1”の状態を活性状態とするならば、即ちValidビットが”0”である行の情報は無効となる。例えばMACアドレス#2のValidビットが”0”であると、K_{2Even}、K_{2Odd}に何が設定されていてもこれらの値は参照されない。

【0059】ステップSP8において否定結果が得られた場合、このことはMRに合致するMACアドレスが鍵テーブル上に存在せず、当該パケットは受信装置21が受信すべきパケットではないことを表しており、復号部34はステップSP13に進み、当該パケットを破棄し、ステップSP14で処理を終了する。

【0060】これに対してステップSP8において肯定結果が得られた場合、このことはMRに合致するMACアドレスが鍵テーブル上に存在し、当該パケットは受信装置21が受信すべきパケットであることを表しており、復号部34はステップSP9に進み、レジスタkにMACアドレスが(1)式の条件下で合致した鍵の索引番号を代入し、ステップSP10へ進む。

【0061】ステップSP10において、復号部34はPSCの上位ビットに基づいて、当該パケットがEven期間の鍵で暗号化されているのかOdd期間の鍵で暗号化されているのかを判断する。例えばPSCの上位ビットが”0”の場合にEven期間、”1”の場合にOdd期間であると定める。

【0062】そして復号部34は、PSCの上位ビットが”0”であった場合は、合致したMACアドレス#iに対応するEven期間の鍵及びK_{iEven}のValidビットの値を鍵テーブルから取り出し、PSCの上位ビットが”1”であった場合は、合致したMACアドレス#iに対応するOdd期間の鍵及びK_{iOdd}のValidビットの値を鍵テーブルから取り出し、次のステップSP11に進む。

【0063】ステップSP11において、復号部34は、取り出したValidビットの値が、”1”であるか(すなわちValid(k,EO)=1)であるかを判断する。ステップSP11において否定結果が得られた場合、このことはValid(k,EO)が”0”であること、すなわちパケットが暗号化されているにもかかわらず有効な復号鍵(個別鍵)が存在しないことを表しており、復号部34はステップSP13に進んで当該パケットを破棄し、ステップSP14で処理を終了する。

【0064】これに対してステップSP11において肯定結果が得られた場合、このことはValid(k,EO)が”1”であること、すなわちパケットに対する有効な復号鍵(個別鍵)が存在することを表しており、復号部34はステップSP12に進む。

【0065】ステップSP12において復号部34は、KEY(k,EO)すなわちk番めのEOに対応する復

号鍵を鍵テーブル37から取り出し、当該復号鍵を用いてパケットを復号して後段のチェッカ35に出力し、ステップSP14で処理を終了する。

【0066】かくして復号部34は、鍵テーブル37及びハッシュテーブルに基づいて、ユニキャスト、マルチキャスト及びブロードキャストの各配信形態に対応したパケット復号処理を行う。

【0067】ここで、かかる復号処理における復号鍵の検索処理(ステップSP5~SP13)は、MACアドレスの弁別処理(ステップSP1~SP4)とは独立に処理されるため、ブロードキャストアドレスに対しても暗号化処理を行うことができる。この場合、共通鍵をブロードキャストアドレスに対する通信の復号鍵とする第1の方法と、ブロードキャストアドレスを個別鍵に対応するMACアドレスとして鍵テーブルへ登録する第2の方法の2つの共通鍵設定方法が考えられる。

【0068】第1の方法では、鍵テーブル37の記憶領域は消費しないが他の同報通信と鍵を共用しなければならない。第2の方法では鍵テーブルの記憶領域を消費するものの、ブロードキャスト専用の復号鍵を設定することができる。

【0069】(5)実施の形態における動作及び効果以上の構成において、復号部34は、受信したデータストリームD31の各パケットに記述されたMACアドレスに基づいて、ブロードキャストアドレス(“0xFFFFFFF”)を有するパケットを弁別するとともに、マスクビットを用いたMACアドレスの照合を行い、マルチキャスト及びユニキャストのパケットを弁別する。このとき復号部34はMACアドレスのハッシュ値を算出し、当該ハッシュ値に基づいてマルチキャスト及びユニキャストのパケット弁別を行う。

【0070】そして復号部34は、弁別されたパケットが暗号化されているかを検出し、当該パケットが暗号化されている場合、復号鍵を鍵テーブルより取り出して復号処理を行う。このとき復号部34はパケットのCKIに基づいて、当該パケットの暗号化が共通鍵によるものか個別鍵によるものかを判別し、これに応じて共通鍵又は個別鍵を用いてパケットを復号する。

【0071】以上の構成によれば、特定のMACアドレスをブロードキャストアドレスとして用いるとともに、マスクビットを用いてMACアドレスの一部のビットのみを照合するようにしたことにより、ブロードキャスト、マルチキャスト及びユニキャストといった様々な受信制御を行うことができる。

【0072】また、ハッシュ関数を用いてMACアドレスのビット数を縮小し、当該縮小したMACアドレスを用いてパケットの弁別を行うようにしたことにより、復号部34の回路規模を縮小することができる。

【0073】(6)他の実施の形態
なお上述の実施の形態においては、マスクビットが”

1”である位置のビットを、MACアドレスの比較対象としたが、本発明はこれに限らず、逆にマスクビットが”0”である位置のビットをMACアドレスの比較対象とするようにしても良い。

【0074】また上述の実施の形態においては、ハッシュテーブルを用いたパケットの弁別において、ハッシュテーブルの検索結果が”0”である場合にパケットを破棄するようにしたが、本発明はこれに限らず、逆にハッシュテーブルの検索結果が”1”である場合にパケットを破棄するようにハッシュテーブルを設定しても良い。

【0075】さらに上述の実施の形態においては、MACアドレス“0xFFFFFFFF”をブロードキャストアドレスとしたが、本発明はこれに限らず、これ以外のMACアドレス“0xFFFFFFFF”をブロードキャストアドレスとしても良い。

【0076】さらに上述の実施の形態においては、復号処理においてブロードキャストアドレスの弁別（ステップSP2）、鍵テーブルにおけるMACアドレスの照合（ステップSP3）、ハッシュテーブルの検索（ステップSP4）の順で処理を行うようにしたが、本発明はこれに限らず、これ以外の順序で復号処理を行うようにしても良い。

【0077】さらに上述の実施の形態においては、衛星データ伝送システムに本発明を適用する場合について述べたが、本発明はこれに限らず、これ以外のデータ伝送システム、例えばケーブルインターネット等に適用しても良い。

【0078】

【発明の効果】 上述のように本発明によれば、受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信

するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにしたことにより、簡易な構成で様々な受信制御を行うことができる。

【図面の簡単な説明】

【図1】 本発明による衛星データ伝送システムの全体構成を示すブロック図である。

【図2】 受信装置の回路構成を示すブロック図である。

【図3】 ヘッドフォーマットを示す略線図である。

【図4】 マスクとMACアドレスの関係を示す略線図である。

【図5】 鍵テーブルのデータ構成を示す略線図である。

【図6】 復号処理を示すフローチャートである。

【符号の説明】

1……衛星データ伝送システム、2……送信側システム、3……衛星、4……受信側システム、5……インターネット、10……制御装置、11……回線接続装置、12……データサーバ、13……送信処理装置、14……ローカルネットワーク、15……送信アンテナ、20……受信アンテナ、21……受信装置、22……情報処理装置、23……回線接続装置、24……ローカルネットワーク、30……CPU、31……フロントエンド部、32……デマルチプレクサ、33……受信フィルタ、34……復号部、35……チェッカ、36……バッファ、37……鍵テーブル、38……インターフェース部、39……バス。

【図2】

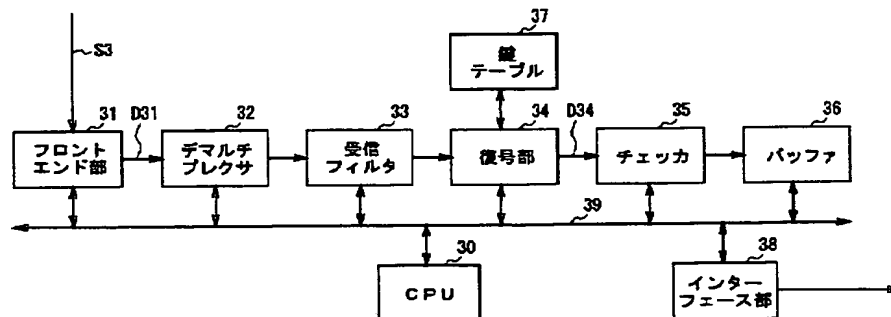


図2 受信装置

【図1】

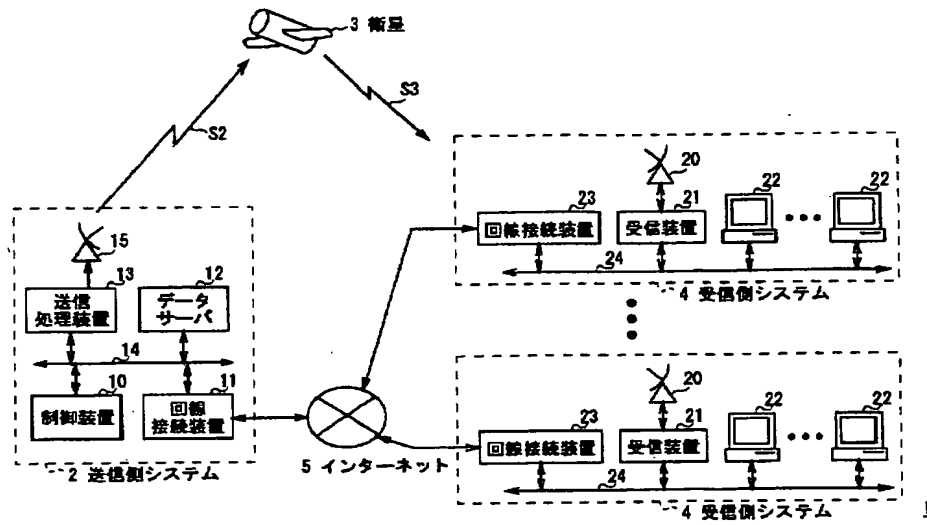


図1 衛星データ伝送システム

【図3】

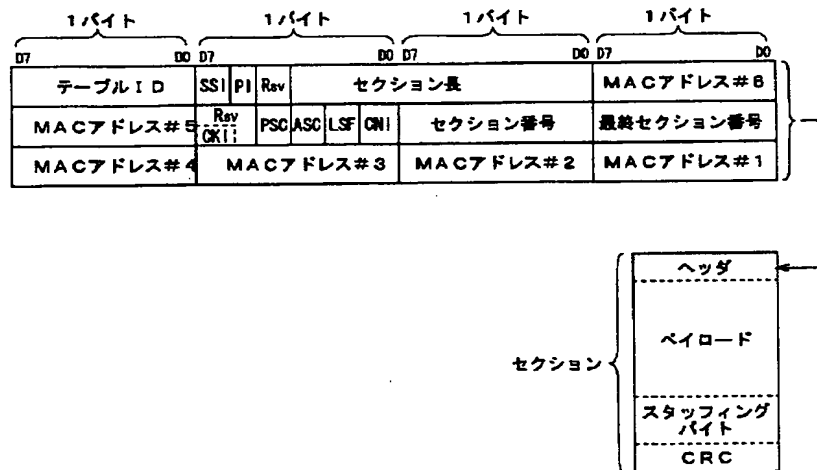


図3 ヘッダフォーマット

【図4】

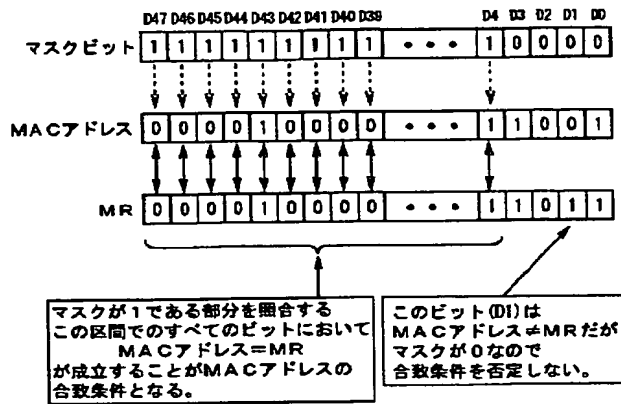


図4 マスクとMACアドレス

【図5】

#1	Valid: MACアドレス #1(48bit)	マスク #1(48bit)	Valid: Known(mbit)	Valid: Known(mbit)
#2	Valid: MACアドレス #2(48bit)	マスク #2(48bit)	Valid: Known(mbit)	Valid: Known(mbit)
#3	Valid: MACアドレス #3(48bit)	マスク #3(48bit)	Valid: Known(mbit)	Valid: Known(mbit)
	⋮		⋮	⋮
#4	Valid: MACアドレス #n(48bit)	マスク #n(48bit)	Valid: Known(mbit)	Valid: Known(mbit)

図5 鍵テーブル

【図6】

